GLASNIK MATEMATIČKI
Vol. 56(76)(2021), 1 – 15

SYMMETRIC 1-DESIGNS FROM $\mathrm{PGL}_2(q)$, FOR q AN ODD PRIME POWER

Xavier Mbaale and Bernardo Gabriel Rodrigues
University of KwaZulu-Natal and University of Pretoria, South Africa

Abstract. All non-trivial point and block-primitive 1-(v, k, k) designs $\mathcal{D}$ that admit the group $G = \mathrm{PGL}_2(q)$, where q is a power of an odd prime, as a permutation group of automorphisms are determined. These self-dual and symmetric 1-designs are constructed by defining $\left\{\frac{|M|}{|M\cap M^g|} : g \in G\right\}$ to be the set of orbit lengths of the primitive action of G on the conjugates of M.

1. Introduction

In [12] (see also [17]) a systematic program to determine symmetric and self-dual 1-designs admitting a prescribed primitive permutation group G has been proposed. Hitherto, many interesting examples of 1-(v, k, k) designs have been obtained from finite primitive permutation groups, see for example [7, 12, 13, 17, 18, 19].

The said program is based on the following result, described in [12, Proposition 1], corrected in [13] and later used in [17].

Result 1.1. *Let G be a finite primitive permutation group acting on the set Ω of size n. Let $\alpha \in \Omega$, and let $\Delta \neq \{\alpha\}$ be an orbit of the stabilizer G_α of α. If $\mathcal{B} = \{\Delta^g \mid g \in G\}$ and, given $\delta \in \Delta$, $\mathcal{E} = \{\{\alpha, \delta\}^g \mid g \in G\}$, then $\mathcal{D} = (\Omega, \mathcal{B})$ forms a symmetric 1-$(n, |\Delta|, |\Delta|)$ design. Further, if Δ is a self-paired orbit of G_α then $\Gamma = (\Omega, \mathcal{E})$ is a regular connected graph of valency $|\Delta|$, $\mathcal{D}$ is self-dual, and G acts as an automorphism group on each of these structures, primitive on vertices of the graph, and on points and blocks of the design.*

2020 *Mathematics Subject Classification.* 05E20, 05E30, 94B05.
Key words and phrases. Symmetric designs, linear code, projective general linear group.

We note that in [5] (see also [6]), Crnković and Mikulić generalized Result 1.1 by proposing a program of construction of 1-designs from finite primitive permutation groups, which are not necessarily symmetric, and whose point- and block-stabilizers are not necessarily conjugate.

In this paper, Result 1.1 is applied to all primitive permutation representations of $G = \mathrm{PGL}_2(q)$, the projective general linear group, for q a power of an odd prime. This paper is motivated by the results obtained in [16] concerning the classification of all symmetric and self-dual 1-(v, k, k) designs admitting $\mathrm{PSL}_2(q)$ for q a power of an odd prime, acting as a point- and block-primitive group of automorphisms of the designs. Since for $q = 2^m \geq 4$, $\mathrm{PGL}_2(q)$ is isomorphic to $\mathrm{PSL}_2(q)$, the designs invariant under $\mathrm{PGL}_2(q)$ for q a power of 2 were examined in [7] and in [19]. Thus, when combined with the results of [7] and of [19], this paper gives a complete account on all non-trivial, symmetric and self-dual 1-(v, k, k) designs admitting G constructed using Result 1.1.

The designs constructed in this paper are given in the following theorem which is proved in the subsequent sections.

Theorem 1.2. *Let $\mathcal{D}$ be a non-trivial symmetric and self-dual* 1-(v, k, k) *design, and let $G = \mathrm{PGL}_2(q)$, where q is a power of an odd prime, be a point- and block-primitive automorphism group of $\mathcal{D}$. Further, let $M \ncong C_p^n \rtimes C_{q-1}$ be a maximal subgroup of G. Then the following hold.*

a) If $M \cong D_{2(q+1)}$ then $\mathcal{D}$ has parameters:
(i) 1-$\left(\frac{q(q-1)}{2}, q+1, q+1\right)$, *or (ii)* 1-$\left(\frac{q(q-1)}{2}, \frac{q+1}{2}, \frac{q+1}{2}\right)$.

b) If $M \cong D_{2(q-1)}$ then $\mathcal{D}$ has parameters:
(i) 1-$\left(\frac{q(q+1)}{2}, 2(q-1), 2(q-1)\right)$, *(ii)* 1-$\left(\frac{q(q+1)}{2}, q-1, q-1\right)$, *or (iii)* 1-$\left(\frac{q(q+1)}{2}, \frac{q-1}{2}, \frac{q-1}{2}\right)$.

c) If $M \cong S_4$ then $\mathcal{D}$ has parameters:
(i) 1-$\left(\frac{q^3-q}{24}, 24, 24\right)$, *(ii)* 1-$\left(\frac{q^3-q}{24}, 12, 12\right)$, *(iii)* 1-$\left(\frac{q^3-q}{24}, 8, 8\right)$, *(iv)* 1-$\left(\frac{q^3-q}{24}, 6, 6\right)$, *or (v)* 1-$\left(\frac{q^3-q}{24}, 4, 4\right)$.

d) If $M \cong \mathrm{PGL}_2(p) \leq \mathrm{PGL}_2(q = p^r)$, where r is an odd prime then $\mathcal{D}$ has parameters:
(i) 1-$\left(\frac{p^r(p^{2r}-1)}{p^3-p}, p^3-p, p^3-p\right)$, *(ii)* 1-$\left(\frac{p^r(p^{2r}-1)}{p^3-p}, p^2-1, p^2-1\right)$, *or (iii)* 1-$\left(\frac{p^r(p^{2r}-1)}{p^3-p}, p(p\pm 1), p(p\pm 1)\right)$.

The paper is organized as follows: in Section 2 we outline the background and notation and give a brief overview on the group $\mathrm{PGL}_2(q)$. In Section 3 we describe the construction method used and give our results on all $\mathrm{PGL}_2(q)$-invariant self-dual, symmetric and primitive 1-designs.

2. Preliminaries

The notation for designs is as in [2]. An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$ is a t-(v, k, λ) *design* if $v = |\mathcal{P}|$, every $B \in \mathcal{B}$ is incident with exactly k points and every t distinct points are together incident with λ blocks. The numbers that occur as the sizes of the intersections of any two distinct blocks are known as intersection numbers of the design $\mathcal{D}$. The design is quasi-symmetric if any two blocks intersect either in x or in y points, for non-negative integers $x \leq y$. A design is called self-orthogonal if the intersection numbers have the same parity as the block size $\bmod p$, where p is the characteristic of the underlying field. The *code* $C_F(\mathcal{D})$ of the design $\mathcal{D}$ over the finite field F is the subspace of $F^{\mathcal{P}}$ spanned by the incidence vectors of the blocks over F. Let v^B denote the incidence vector of a block $B \in \mathcal{B}$, then $C_F(\mathcal{D}) = \langle v^B | B \in \mathcal{B} \rangle$.

Let $GF(q)$ denote the Galois field with q elements and $X := GF(q) \cup \{\infty\}$, where ∞ is a symbol not in $GF(q)$. Then we can define a fractional linear transformation $T \colon X \to X$ by

$$T \colon x \mapsto \frac{\alpha x + \beta}{\gamma x + \delta}, \qquad \alpha, \beta, \gamma, \delta \in GF(q),$$

such that $\alpha\delta - \beta\gamma$ is a non-zero square in $GF(q)$ and $T(\infty) = \frac{\alpha}{\gamma}$, $T(\frac{-\delta}{\gamma}) = \infty$, if $\gamma \neq 0$, $T(\infty) = \infty$ if $\gamma = 0$ and $T(x) \in GF(q)$ for all $x \in GF(q)$ such that $\gamma x + \delta \neq 0$. Then the set of all such fractional linear transformations forms a group under composition known as the *Projective General Linear Group* of degree 2 over $GF(q)$ and denoted $\mathrm{PGL}_2(q)$. The group $\mathrm{PGL}_2(q)$ has order $q(q^2-1)$. The structure of $\mathrm{PGL}_2(q)$ is well known and can be found in [4, 9, 15].

The following results give the description of the structures of the maximal subgroups of $\mathrm{PGL}_2(q)$ for q a power of an odd prime.

Proposition 2.1 ([1, Proposition 2.1] and [15, Corollary 2.3]). *Let $G = \mathrm{PGL}_2(q)$, with $q = p^n > 3$ for some odd prime p. Then the maximal subgroups of G not containing $\mathrm{PSL}_2(q)$ are:*

- (i) $C_p^n \rtimes C_{q-1}$, *the stabilizer of a point of the projective line;*
- (ii) $D_{2(q+1)}$*;*
- (iii) $D_{2(q-1)}$ *for $q \neq 5$;*
- (iv) S_4 *for $q = p \equiv \pm 3 \pmod 8$;*
- (v) $\mathrm{PGL}_2(p)$ *for $q = p^r$ where r is an odd prime.*

More information concerning $\mathrm{PGL}_2(q)$ can be obtained from $\mathrm{PSL}_2(q)$ since $\mathrm{PGL}_2(p)$ is a subgroup of $\mathrm{PSL}_2(p^2)$.

The elements of $\mathrm{PGL}_2(q)$ are distinguished as follows.

LEMMA 2.2 ([4, Theorem 1]). *Let g be a non-trivial element of* $\mathrm{PGL}_2(q)$ *of order d and with f fix points. Then either $d \mid p^n+1$ and $f=0$, $d=p$ and $f=1$, or $d \mid p^n-1$ and $f=2$.*

A subgroup A of a group G is a trivial intersection (TI) subgroup if for all $g \in G, A \cap A^g = A$ or $A \cap A^g = \{1_A\}$. The group $\mathrm{PGL}_2(q)$ has the following trivial intersection subgroups.

THEOREM 2.3 ([8, Chapter XII], [4, Theorem 2]).

i) Let P be a Sylow p-subgroup of $\mathrm{PGL}_2(q)$ of order p^n. Then every non-trivial element of P has a single fix point and P is a TI-subgroup.
ii) Let H be a cyclic subgroup of $\mathrm{PGL}_2(q)$ of order p^n-1. Then every non-trivial element of H fixes two points. Further, there is no element of $\mathrm{PGL}_2(q) \backslash H$ that fixes these points and so H is a TI-subgroup.
iii) Let K be a cyclic subgroup of $\mathrm{PGL}_2(q)$ of order p^n+1. Then K contains all elements that have no fix point in $\mathrm{PGL}_2(q)$ and K is a TI-subgroup.

REMARK 2.4 ([8, Chapter XII], [4, Theorem 2]). The group G has p^n+1 subgroups of type P with $p^{2n}-1$ distinct fractional linear transformations that fix a point, $\frac{p^n(p^n+1)}{2}$ subgroups of type H with $\frac{p^n(p^n+1)(p^n-2)}{2}$ distinct fractional linear transformations that fix two points and $\frac{p^n(p^n-1)}{2}$ subgroups of type K with $\frac{p^{2n}(p^n-1)}{2}$ distinct fractional linear transformations that do not fix any point.

Let M be a maximal subgroup of G, then G acts by conjugation on the set $\mathcal{M}$ of all conjugates of M in G. We use this action of G on $\mathcal{M}$ to construct primitive symmetric 1-designs admitting G as a permutation group of automorphisms. This is based on the following result.

THEOREM 2.5 ([20, Proposition 2.1]). *Let G be a finite group with a maximal subgroup M. Then the action of G by conjugation on the set $\mathcal{M}$ of left (right) cosets of M in G is primitive.*

For a maximal subgroup M of a group G we adopt the definition of $\mathcal{A}_M$ given in [18], i.e.,

$$\mathcal{A}_M = \{|M \cap M^g| : \ g \in G\}.$$

Note that $\mathcal{A}_M \neq \varnothing$ since $|M| \in \mathcal{A}_M$ for all $g \in M$.

The following lemma gives the lengths of the orbits when G acts on $\mathcal{M}$.

LEMMA 2.6. *Let $\mathcal{M}$ be a set of conjugates of a maximal subgroup M (not normal in G) and G be a finite permutation group that acts primitively on $\mathcal{M}$. Then the lengths of the orbits of this action are given by:*

$$\left\{\frac{|M|}{l} : l \in \mathcal{A}_M\right\}, \textit{where } \mathcal{A}_M \textit{ is as defined above.}$$

PROOF. The proof follows from [18, Lemma 3.3], since M is maximal and not normal in G, then $N_G(M) = M$. ∎

REMARK 2.7. It follows from Lemma 2.6 that in order to find the orbit lengths for the action given in Result 1.1, one needs to explicitly determine the set $\mathcal{A}_M$.

3. CONSTRUCTING OF SYMMETRIC 1-DESIGNS

In the sequel, for M a maximal subgroup of $\mathrm{PGL}_2(q)$, where $q = p^n$, p is an odd prime and $n \in \mathbb{N}$, as described in Proposition 2.1 we consider the conjugacy class of maximal subgroups conjugate to M and determine $\mathcal{A}_M$ with a view to construct all $\mathrm{PGL}_2(q)$-invariant self-dual, primitive and symmetric 1-designs. We start by making the following observations on the conjugacy classes of involutions of $\mathrm{PGL}_2(q)$.

REMARK 3.1. We shall consider the elements of $G = \mathrm{PGL}_2(q)$ as permutations on the set $X := GF(q) \cup \{\infty\}$ and say that an element of X is of even or odd type if as a permutation it has even or odd parity.

The group G has two conjugacy classes of involutions, one of even type and another of odd type. In particular, it follows from [3, Section 2] that for $q \equiv 1 \pmod 4$ the centralizer of an involution of even type has order $2(q-1)$, while the centralizer of an involution of odd type has order $2(q+1)$. Furthermore, when $q \equiv 3 \pmod 4$ the centralizer of an involution of even type has order $2(q+1)$, and that of an involution of odd type has order $2(q-1)$. Thus, when $q \equiv 1 \pmod 4$, G has $\frac{q(q+1)}{2}$ involutions of even type, and $\frac{q(q-1)}{2}$ involutions of odd type, and when $q \equiv 3 \pmod 4$, G has $\frac{q(q-1)}{2}$ involutions of even type, and $\frac{q(q+1)}{2}$ involutions of odd type, respectively.

We note that for $M \cong C_p^n \rtimes C_{q-1}$, the set $\mathcal{M}$ has $q+1$ points on which G acts 2-transitively. Under this action the designs constructed from M using Result 1.1 are trivial and thus of no interest for classification purposes.

To this end we start by considering M to be a maximal subgroup isomorphic to the dihedral group $D_{2(q\pm1)}$ in G. We show in Theorem 3.4 that for all $g \in G\backslash M$, $|M \cap M^g| \in \{2, 4\}$ whenever $M \cong D_{2(q+1)}$. Subsequently, in Theorem 3.6 we prove that $|M \cap M^g| \in \{1, 2, 4\}$ whenever $M \cong D_{2(q-1)}$. Observe that for $M \cong D_{2(q\pm1)}$ and $g \in G\backslash M$ it was proved in [16, Lemma 3.5] that every $x \in M \cap M^g$ is an involution. So, we need only to describe the nature of the elements that occur in the intersections $M \cap M^g$ of size four, and this is done in the next result.

LEMMA 3.2. *Let* $M \cong D_{2(q\pm1)} = \langle s, r : r^{q\pm1} = s^2 = 1_M, srs^{-1} = r^{-1}\rangle$ *be a maximal subgroup of* G. *Suppose that* $r^{\frac{q\pm1}{2}}$ *and* sr^i *have the same parity. Then there exists* $g \in G\backslash M$ *such that* $M \cap M^g = \{r^{\frac{q\pm1}{2}}, sr^i, sr^{\frac{2i+q\pm1}{2}}, 1_M\}$, *where* $1 \le i \le q \pm 1$.

PROOF. Note that Remark 3.1 implies that all involutions with the same parity in G are in the same conjugacy class. Thus for $r^{\frac{q\pm1}{2}}$ in M, there exists

$g \in G \backslash M$ such that $\left(r^{\frac{q\pm1}{2}}\right)^g = sr^i \in M \cap M^g$, for $1 \leq i \leq q \pm 1$. Note also that $sr^{\frac{q\pm1}{2}}$ is in M and

$$\left(sr^{\frac{q\pm1}{2}}\right)^g = s^g \left(r^{\frac{q\pm1}{2}}\right)^g = s^g(sr^i) = sr^j sr^i = r^{-j}r^i, \quad 1 \leq j \leq q \pm 1.$$

This forces $i - j = \frac{q\pm1}{2}$, and from this we obtain that $r^{-j}r^i$ is an involution, so that $\left(sr^{\frac{q\pm1}{2}}\right)^g = r^{\frac{q\pm1}{2}} \in M \cap M^g$. Hence for $g \in G \backslash M$ we must have $M \cap M^g = \{r^{\frac{q\pm1}{2}}, sr^i, sr^{\frac{2i+q\pm1}{2}}, 1_M\}$, where $1 \leq i \leq q \pm 1$. Notice that $\frac{2i+q\pm1}{2}$ is taken modulo $q \pm 1$. $\square$

Before we prove the next theorem, we need the following lemma.

Lemma 3.3. *Let $k \neq 1, 2$ be such that k divides $q \pm 1$. Then the number of elements in G of order k is equal to $\frac{\phi(k)q(q\mp1)}{2}$ where ϕ is the Euler's phi-function.*

Proof. The proof is similar to that given for [16, Lemma 3.8]. However, for the reader's benefit we sketch the arguments here. Let H be a cyclic subgroup of G of order $q \pm 1$. By [8, pp. 242–243], $N_G(H) = D_{2(q\pm1)}$. Further, if S is a subgroup of H, then $N_G(S) = D_{2(q\pm1)}$. Let $k \neq 1, 2$ be such that k divides $q \pm 1$. Then the number of elements in G of order k equals

$$[G : N_G(S)]\phi(k) = \frac{q(q-1)(q+1)\phi(k)}{2(q\pm1)} = \frac{\phi(k)q(q\mp1)}{2}.$$

$\square$

We are now ready to determine the set $\mathcal{A}_M$ starting with $M \cong D_{2(q+1)}$.

Theorem 3.4. *Let $M \cong D_{2(q+1)}$ be a maximal subgroup of G. Then for all $g \in G \backslash M$, $|M \cap M^g| \in \{2, 4\}$.*

Proof. We first note that the number of distinct conjugates of M in G is $\frac{q(q-1)(q+1)}{2(q+1)} = \frac{q(q-1)}{2}$. Thus the number of distinct intersections $M \cap M^g$ equals $\frac{q(q-1)}{2} - 1 = \frac{(q-2)(q+1)}{2}$. From [16, Theorem 3.10] we have that if $\{1_G\} \neq M \cap M^g \leq M$ then $M \cap M^g \cong C_2$ or $M \cap M^g \cong C_2 \times C_2$. We will show that these are the only possibilities. The proof follows by a counting argument on the types of involutions and the possible sizes of their intersections. To this end we consider the following two cases:

Case 1: Suppose $q + 1 \equiv 0 \pmod 4$. By Remark 3.1, G has $\frac{q(q-1)}{2}$ involutions of even type and $\frac{q(q+1)}{2}$ involutions of odd type, respectively. From this we infer that M has $\frac{q+1}{2}$ involutions of odd type, and $\frac{q+1}{2} + 1 = \frac{q+3}{2}$ involutions of even type. Therefore each involution of odd type in G is contained in

$$\frac{\left(\frac{q(q-1)}{2}\right)\left(\frac{q+1}{2}\right)}{\frac{q(q+1)}{2}} = \frac{q-1}{2}$$

distinct conjugates M^g of M. Similarly each involution of even type in G is contained in

$$\frac{\left(\frac{q(q-1)}{2}\right)\left(\frac{q+3}{2}\right)}{\frac{q(q-1)}{2}} = \frac{q+3}{2}$$

distinct conjugates of M. Now from Lemma 3.2 we observe that the involution $r^{\frac{q+1}{2}}$ occurs in every intersection $M \cap M^g$ of size four. Notice further that this is an involution of even type, since it has $\frac{q+1}{2}$ transpositions. Since the preceding paragraph shows that an involution of even type is in $\frac{q+3}{2}$ distinct conjugates of M in G we deduce that the number of intersections $M \cap M^g$ of size four is $\frac{q+3}{2} - 1$.

To determine the number of intersections $M \cap M^g$ of size two we first note that all involutions in intersections $M \cap M^g$ of size four are of even type. Since there are $\frac{q+1}{2}$ intersections of size four, these must account for $2 \times \frac{q+1}{2}$ involutions of even type in M (notice that the involution $r^{\frac{q+1}{2}}$ that occurs in all intersections $M \cap M^g$ of size four is excluded). This shows that each involution of even type in M occurs in two intersections $M \cap M^g$ of size four (since M has precisely $\frac{q+1}{2}$ involutions of even type after excluding the involution $r^{\frac{q+1}{2}}$). Since the involutions of even type in G occur in $\frac{q+3}{2}$ distinct conjugates M^g of M we must have that the number of intersections $M \cap M^g$ of size two consisting of involutions of even type from M equals $\left(\frac{q+3}{2} - 3\right)\left(\frac{q+1}{2}\right)$.

Therefore, the total number of intersections $M \cap M^g$ of size two is $\left(\frac{q-1}{2} - 1\right)\left(\frac{q+1}{2}\right)$, and these consist of involutions of odd type together with $\left(\frac{q+3}{2} - 3\right)\left(\frac{q+1}{2}\right)$ involutions of even type. Adding the $\frac{(q+1)(q-3)}{2}$ intersections $M \cap M^g$ of size two to the $\frac{q+1}{2}$ intersections $M \cap M^g$ of size four we obtain $\frac{(q+1)(q-2)}{2}$ which is the total number of distinct intersections $M \cap M^g$.

Case 2: Suppose $q+1 \equiv 2 \pmod 4$. By Remark 3.1, in G there are $\frac{q(q-1)}{2}$ involutions of odd type and $\frac{q(q+1)}{2}$ involutions of even type respectively. Furthermore, M has $\frac{q+1}{2}$ involutions of even type, and $\frac{q+1}{2} + 1 = \frac{q+3}{2}$ involutions of odd type. Thus each involution of even type in G is in

$$\frac{\left(\frac{q(q-1)}{2}\right)\left(\frac{q+1}{2}\right)}{\frac{q(q+1)}{2}} = \frac{q-1}{2}$$

distinct conjugates of M, and each involution of odd type in G is in

$$\frac{\left(\frac{q(q-1)}{2}\right)\left(\frac{q+3}{2}\right)}{\frac{q(q-1)}{2}} = \frac{q+3}{2}$$

distinct conjugates of M.

Now, since $\frac{q+1}{2}$ is odd, it follows that the involution $r^{\frac{q+1}{2}}$ has an odd number of transpositions. Hence it is an involution of odd type. Arguing as in Case 1, we obtain that the number of intersections $M \cap M^g$ of size four equals $\frac{q+3}{2} - 1$.

We now determine the number of intersections $M \cap M^g$ of size two. Observe that by Lemma 3.2 the elements $r^{\frac{q\pm1}{2}}$ and sr^i are of the same parity. By the preceding discussion we infer that these involutions are of odd type. Furthermore, the element $sr^{\frac{2i+q\pm1}{2}}$ is an involution of even type since it is the product of two involutions of odd type. Since there are $\frac{q+1}{2}$ intersections $M \cap M^g$ of size four, this accounts for $\frac{q+1}{2}$ involutions of odd type and $\frac{q+1}{2}$ involutions of even type, respectively in M. We have thus shown that each involution of M except $r^{\frac{q\pm1}{2}}$ occurs in exactly one intersection $M \cap M^g$ of size four. The total number of intersections $M \cap M^g$ of size two is obtained by adding $\left(\frac{q+3}{2} - 2\right) \times \left(\frac{q+1}{2}\right)$ involutions of odd type to $\left(\frac{q-1}{2} - 2\right)\left(\frac{q+1}{2}\right)$ involutions of even type. Hence, adding the total number of distinct intersections $M \cap M^g$ of size four and size two respectively we obtain $\frac{(q+1)(q-2)}{2}$ as expected. Therefore $|M \cap M^g| \in \{2, 4\}$, for all $g \in G \setminus M$. ∎

As an immediate consequence of Lemma 2.6 and Theorem 3.4 we deduce the following.

Corollary 3.5. *Let $M = D_{2(q+1)}$ be a maximal subgroup of G and $\mathcal{M}$ be the set of conjugates of M in G on which G acts by conjugation. Then the primitive action of G on $\mathcal{M}$ has one non-trivial orbit of length $\frac{q+1}{2}$ and $\frac{q-3}{2}$ orbits of length $q+1$.*

Proof. This follows directly from Lemma 2.6 and Theorem 3.4. ∎

The following theorem determines the set $\mathcal{A}_M$ when $M \cong D_{2(q-1)}$.

Theorem 3.6. *Let $M \cong D_{2(q-1)}$ be a maximal subgroup of G. Then $|M \cap M^g| \in \{1, 2, 4\}$ for all $g \in G \backslash M$.*

Proof. The proof that there are intersections $M \cap M^g$ of sizes two and four, respectively follows using similar arguments to those given in the proof of Theorem 3.4. So, we need only prove that there are intersections $M \cap M^g$ of size one. We note first that the number of distinct conjugates of M in G is $\frac{q(q-1)(q+1)}{2(q-1)} = \frac{q(q+1)}{2}$. So, the number of distinct intersections $M \cap M^g$ equals $\frac{q(q+1)}{2} - 1 = \frac{q(q+1)-2}{2}$. Recall that by [16, Theorem 3.10], we have that if $\{1_G\} \neq M \cap M^g$ then either $M \cap M^g \cong C_2$ or $M \cap M^g \cong C_2 \times C_2$. We consider the following cases:

Case 1: Suppose $q - 1 \equiv 0 \pmod 4$. Arguing as in Case 1 of Theorem 3.4, we can show that there are $\frac{q-1}{2}$ intersections $M \cap M^g$ of size four and $\frac{(q-1)(q-3)}{2}$ intersections $M \cap M^g$ of size two, respectively. But observe that

$$\frac{q-1}{2} + \frac{(q-1)(q-3)}{2} = \frac{(q-1)(q-2)}{2} < \frac{q(q+1)}{2} - 1.$$

So there exists $g \in G\backslash M$ such that $M \cap M^g = \{1_G\}$.

CASE 2: Suppose $q-1 \equiv 2 \pmod 4$. Arguing as in Case 2 of Theorem 3.4, it can be shown that there are $\frac{q-1}{2}$ intersections $M \cap M^g$ of size four and $\frac{(q-1)(q-3)}{2}$ intersections $M \cap M^g$ of size two. Since

$$\frac{q-1}{2} + \frac{(q-1)(q-3)}{2} = \frac{(q-1)(q-2)}{2} < \frac{q(q+1)}{2} - 1$$

we deduce that there exists $g \in G\backslash M$ such that $M \cap M^g = \{1_G\}$. □

We now deduce the following.

COROLLARY 3.7. *Let $M = D_{2(q-1)}$ be a maximal subgroup of G and $\mathcal{M}$ be the set of conjugates of M in G on which G acts by conjugation. Then the primitive action of G on $\mathcal{M}$ has one non-trivial orbit of length $\frac{q-1}{2}$, $\frac{q-3}{2}$ orbits of length $q-1$ and one orbit of length $2(q-1)$.*

PROOF. For the proof use Lemma 2.6 and Theorem 3.6. □

In the following remark, we give a geometric description of the orbits given in Corollary 3.7.

REMARK 3.8. Since $G = \mathrm{PGL}_2(q)$ acts naturally on the $q+1$ points of $X := GF(q) \cup \{\infty\}$, one can also obtain geometrically the orbit lengths given in Corollary 3.7. It is known that G acts primitively on unordered pairs of points of X i.e, $X^{\{2\}}$ of degree $\binom{q+1}{2}$. Let H be the stabilizer of a pair $\{0, \infty\}$ as a point. While considering $\mathrm{PSL}_2(2^m) \cong \mathrm{PGL}_2(2^m)$, for some m, Darafsheh in [7, Proposition 2] showed that $H \cong D_{2(q-1)}$ and the orbits of H on $X^{\{2\}}$ are: $\{0, \infty\}$ of length 1, $\{\{0, b\} \cup \{\infty, c\} \,|\, b, c \in GF(q)^*\}$ of length $2(q-1)$, $\{\{\lambda b, \lambda c\} \,|\, b, c, \lambda \in GF(q)^*\}$ of length $q-1$ and lastly $\{\{\lambda, \lambda(q-1)\} \,|\, \lambda \in GF(q)^*\}$ of length $\frac{q-1}{2}$.

In the following theorem, we prove that the 1-design $\mathcal{D}$ obtained by taking for block set the images under G of the orbit of length $2(q-1)$ is quasi-symmetric and self-orthogonal.

THEOREM 3.9. *Let $\mathcal{D}$ be the 1-$\left(\frac{q(q+1)}{2}, 2(q-1), 2(q-1)\right)$ design obtained by taking for blocks the images under G of the orbit of length $2(q-1)$. Then $\mathcal{D}$ is a quasi-symmetric and self-orthogonal design, with block intersection numbers 4 and $q-1$, respectively.*

PROOF. We first note that blocks of $\mathcal{D}$ are determined by the pair of points of $X^{\{2\}}$ being stabilized by elements of a maximal subgroup $M \cong D_{2(q-1)}$. Notice that if the pair being stabilized by M is $\{0, \infty\}$, then we have a block of length $2(q-1)$ given by

$$\{\{0, b\} \cup \{\infty, c\} \,|b, c \in GF(q)^*\}$$

i.e, a set of all pairs in $X^{\{2\}}$ with each pair having exactly one element in $\{0, \infty\}$. However, if the point being stabilized by M is $\{a, b\}, a, b \in GF(q)^*$ then its block is defined by

$$\overline{\{a, b\}} := \{\{a, \alpha_1\} \cup \{b, \alpha_2\} \,|\, \alpha_1, \alpha_2 \in X \backslash \{a, b\}\}.$$

Let $a, b, c, d \in X$ such that $\overline{\{a, b\}}, \overline{\{c, d\}}$ and $\overline{\{a, c\}}$ are blocks as defined above where $a \neq b \neq c \neq d$. Then

$$\overline{\{a, b\}} \cap \overline{\{c, d\}} = \{\{a, d\}, \{a, c\}, \{b, d\}, \{b, c\}\}.$$

Also,

$$\overline{\{a, b\}} \cap \overline{\{a, c\}} = \{\{b, c\} \cup \{i, a\} \,|\, i \in X \backslash \{a, b, c\}\}$$

is of size $1 + (q + 1 - 3) = q - 1$. Since q is a power of an odd prime, $q - 1 \equiv 0 \pmod 4$ and so $2(q-1) \equiv 0 \pmod 2$. Hence $\mathcal{D}$ is self-orthogonal. ∎

REMARK 3.10.

a) The codes obtained from the binary row span of $\mathcal{D}$ are isomorphic to the binary codes of the triangular graph, and have been examined in [14] with a view to permutation decoding. Note that the codes are self-orthogonal and doubly-even with parameters

$$\left[\frac{q(q+1)}{2}, q-1, 2(q-1)\right]_2.$$

b) The design $\mathcal{D}$ in Theorem 3.9 is neither a 2-design, nor a t-design for $t \geq 3$. For a t-(v, k, λ) design, every s-subset of points ($s \leq t$) is contained in exactly $\lambda_s = \frac{(v-s)}{(k-s)}\lambda_{s+1}$ blocks, for $0 \leq s \leq t-1$. Denote $\lambda_t = \lambda, \lambda_0$ (the total number of blocks) by b, and (if $t \geq 1$) to denote λ_1 (the number of blocks containing a point) by r. Using the above equality and the parameters for the design $\mathcal{D}$ in Theorem 3.9, we have

$$\lambda_2 = \frac{(2q-2)(2q-3)}{\frac{q(q+1)}{2} - 1} = \frac{8q-12}{q+2}.$$

Since for all q, λ_2 is not an integer, the first part of the claim follows. The second part of the claim follows by noticing that if $\mathcal{D}$ is a 3-design, then it is a 2-design.

We now determine the set $\mathcal{A}_M$ for M a maximal subgroup of $\mathrm{PGL}_2(q)$ isomorphic to S_4.

THEOREM 3.11. *Let $M \cong S_4$ be a maximal subgroup of $G = \mathrm{PGL}_2(q)$ for $q = p \equiv \pm 3 \pmod 8$. Then $|M \cap M^g| \in \{1, 2, 3, 4, 6, 24\}$ for all $g \in G$.*

PROOF. Notice first that the number of distinct conjugates of M in G is $\frac{q(q^2-1)}{24}$. So, the number of distinct intersections $M \cap M^g$ equals $\frac{q(q^2-1)}{24} - 1$. To show that $|M \cap M^g| \in \{1, 2, 3, 4, 6, 24\}$, we evaluate the possible sizes of the intersections $M \cap M^g$ recalling that $M \cap M^g \leq S_4$. We start by showing that $|M \cap M^g| \notin \{12, 8\}$. Suppose that $|M \cap M^g| = 12$. Then there must exist

$g \in G \setminus M$ such that $M \cap M^g \cong A_4$. But this is a contradiction since we have $N_G(A_4) \cong S_4$ by [11, Table on page 4 and Proposition 3.4].

Next, suppose that $|M \cap M^g| = 8$. Then $M \cap M^g \cong D_8$, and by [11, Theorem 1.5] it follows that $N_G(D_8) \cong D_{16}$, and moreover $D_{16} \leq G$ only if $q = p \equiv \pm 1 \pmod 8$. Since D_{16} is not a subgroup of G for $q = p \equiv \pm 3 \pmod 8$, this implies that there is no $g \in G$ for which $|M \cap M^g| = 8$.

Now, for every $g \in M$ we have $|M \cap M^g| = 24$, so we must have that $24 \in \mathcal{A}_M$.

If $|M \cap M^g| = 6$, then $M \cap M^g \cong S_3$. By [11, Theorem 1.5] we have $N_G(S_3) = D_{12}$. Since D_{12} is a subgroup of G if $q = p \equiv \pm 1 \pmod 6$, and since all primes q that satisfy $q = p \equiv \pm 3 \pmod 8$ are congruent $\pm 1 \pmod 6$, there must exist $g \in G$ such that $M \cap M^g \cong S_3$.

Recall that up to isomorphism S_4 has only four subgroups of order 3. This shows that there are only four distinct intersections $M \cap M^g$ of size six.

Suppose now that $|M \cap M^g| = 4$. Then either $M \cap M^g \cong C_2 \times C_2$ or $M \cap M^g \cong C_4$. But [10, Theorem 1.3 (iv)] rules out the possibility that $M \cap M^g \cong V_4$ since $N_G(V_4) \cong S_4$. Hence $M \cap M^g \cong C_4$.

Since S_4 has six elements of order 4 and since by Lemma 3.3, G has $q(q \pm 1)$ elements of order 4, i.e., $q(q+1)$ if $q \equiv 1 \pmod 4$ and $q(q-1)$ if $q \equiv 3 \pmod 4$, we deduce that each element of order 4 in G is in

$$\frac{6\left(\frac{q^3-q}{24}\right)}{q(q \pm 1)} = \frac{q \mp 1}{4}$$

distinct conjugates M^g of M. Thus there are

$$\frac{6\left(\frac{q \mp 1}{4} - 1\right)}{2} = 3\left(\frac{q \mp 1}{4} - 1\right)$$

intersections $M \cap M^g$ of size four.

Observe that S_4 has eight elements of order 3, and four subgroups of order 3. Since by Lemma 3.3, G has $q(q \pm 1)$ elements of order 3, and each element of order 3 in G is in $\frac{8\left(\frac{q^3-q}{24}\right)}{q(q\pm 1)} = \frac{q \mp 1}{3}$ distinct conjugates of M we conclude that there are $4(\frac{q \mp 1}{3} - 1)$ intersections $M \cap M^g$ containing an element of order 3. From the above discussion we observe that four of these intersections have order 6. So the number of intersections $M \cap M^g$ of size three is $4(\frac{q \mp 1}{3} - 1) - 4$.

Finally, since S_4 has 6 involutions of odd type, and 3 involutions of even type, we infer that each involution of odd type in G is in

$$\frac{6\left(\frac{q^3-q}{24}\right)}{\frac{q(q \pm 1)}{2}} = \frac{q \mp 1}{2}$$

conjugates M^g, i.e, $\frac{q+1}{2}$ if $q \equiv 1 \pmod 4$ and $\frac{q-1}{2}$ if $q \equiv 3 \pmod 4$ respectively. Similarly, each involution of even type in G is in

$$\frac{3\left(\frac{q^3-q}{24}\right)}{\frac{q(q\pm1)}{2}} = \frac{q \mp 1}{4}$$

distinct conjugates of M, namely $\frac{q-1}{4}$, if $q \equiv 1 \pmod 4$, and $\frac{q+1}{4}$, if $q \equiv 3 \pmod 4$. Thus involutions of odd type are in $6\left(\frac{q\mp1}{2} - 1\right)$ intersections $M \cap M^g$, and involutions of even type are in $3\left(\frac{q\mp1}{4} - 1\right)$ intersections $M \cap M^g$. But recall that some of these intersections with involutions have cardinality six or four. Subtracting the intersections $M \cap M^g$ of size six and four respectively, from the total number of intersections $M \cap M^g$ containing an involution we obtain

$$\begin{aligned}&\left[6\left(\frac{q\pm1}{2} - 1\right) + 3\left(\frac{q\pm1}{4} - 1\right)\right] - \left[3\left(\frac{q\pm1}{4} - 1\right) + 12\right]\\ &\qquad = 6\left(\frac{q\pm1}{2} - 1\right) - 12\end{aligned}$$

which is the number of intersections $M \cap M^g$ of size two.

Since

$$\left(6\left(\frac{q\pm1}{2} - 1\right) - 12\right) + 3\left(\frac{q\mp1}{4} - 1\right) + \left(4\left(\frac{q\mp1}{3} - 1\right) - 4\right) + 4 < \frac{q^3-q}{24} - 1,$$

there must exist $g \in G$ such that $M \cap M^g = \{1_G\}$. ∎

Thus we have

Corollary 3.12. *Let $M \cong S_4$ be a maximal subgroup of G and $\mathcal{M}$ be the set of conjugates of M in G on which G acts by conjugation. Then the primitive action of G on $\mathcal{M}$ has the following non-trivial orbit lengths:*

a) one orbit of length four,
b) $\frac{1}{2} \times \left[\frac{q\pm1}{4} - 1\right]$ orbits of length six,
c) $\frac{1}{2} \times \left[\left(\frac{q\mp1}{3} - 1\right) - 1\right]$ orbits of length eight,
d) $\left[\frac{1}{2} \times \left(\frac{q\pm1}{2} - 1\right)\right] - 1$ orbits of length twelve,
e) $\frac{\left(\frac{q^3-q}{24}-1\right) - \left[\left(6\left(\frac{q\pm1}{2}-1\right)-12\right)+3\left(\frac{q\mp1}{4}-1\right)+\left(4\left(\frac{q\mp1}{3}-1\right)-4\right)+4\right]}{24}$ orbits of length twenty four.

Proof. The proof follows by applying Lemma 2.6 and Theorem 3.11. ∎

Finally, we consider the maximal subgroup $\mathrm{PGL}_2(p)$ of $\mathrm{PGL}_2(q = p^r)$, where r is an odd prime.

Theorem 3.13. *Let $M \cong \mathrm{PGL}_2(p) \leq \mathrm{PGL}_2(q = p^r)$, where r is an odd prime. Then $|M \cap M^g| \in \{1, p-1, p, p+1, |M|\}$ for all $g \in G$.*

PROOF. If $g \in M$, then $M \cap M^g = M$. Every $x \in M$ and consequently every $x \in G$ is in one of the subgroups of types P, H or K of G described in Theorem 2.3. Since these are all TI-subgroups in G, there exists some $g \in G$ such that $|M \cap M^g| \in \{p, p \pm 1\}$.

By Remark 2.4, the subgroup M of G has $p^2 - 1$ elements of order p and G has $p^{2r} - 1$ elements of order p. Each element of order p in G is in

$$\frac{\frac{p^r(p^r+1)(p^r-1)}{p(p-1)(p+1)}\left(p^2-1\right)}{p^{2r}-1} = p^{r-1}$$

conjugates M^g. Thus the number of intersections $M \cap M^g$ of size p is

$$\frac{(p^{r-1}-1)(p^2-1)}{p-1} = (p^{r-1}-1)(p+1).$$

Direct calculations using Remark 2.4 show that M has $\frac{p(p+1)}{2}$ cyclic subgroups of order $p-1$. So M also has $\frac{p(p+1)}{2}$ elements of the form $x = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}$, where ω is a primitive root in $GF(p)$, and x generates a cyclic group of order $p-1$. Further, G has $\frac{p^r(p^r+1)}{2}$ elements that generate cyclic subgroups of order $p-1$. Thus each $x \in G$ is in

$$\frac{\frac{p^r(p^r+1)(p^r-1)}{p(p-1)(p+1)}\left(\frac{p(p+1)}{2}\right)}{\frac{p^r(p^r+1)}{2}} = \frac{p^r-1}{p-1}$$

conjugates of M. From Remark 2.4, we have that M has $\frac{p(p+1)(p-2)}{2}$ elements of order $p-1$. Hence

$$\frac{\left(\frac{p^r-1}{p-1}-1\right)\left(\frac{p(p+1)(p-2)}{2}\right)}{p-2} = \frac{p^2(p+1)(p^{r-1}-1)}{2(p-1)}$$

of the intersections $M \cap M^g$ are of size $p-1$.

It follows by using Remark 2.4 that M has $\frac{p(p-1)}{2}$ elements that generate cyclic subgroups of order $p+1$ while G has $\frac{p^r(p^r-1)}{2}$ elements that generate cyclic subgroups of order $p+1$. Each of the elements of G that generate cyclic subgroups of order $p+1$ occur in

$$\frac{\frac{p^r(p^r+1)(p^r-1)}{p(p-1)(p+1)}\left(\frac{p(p-1)}{2}\right)}{\frac{p^r(p^r-1)}{2}} = \frac{p^r+1}{p+1}$$

conjugates of M. Once again use of Remark 2.4 shows that M has $\frac{p(p-1)}{2}$ elements of order $p+1$. From this we deduce that

$$\frac{\left(\frac{p^r+1}{p+1}-1\right)\left(\frac{p^2(p-1)}{2}\right)}{p} = \frac{p^2(p-1)(p^{r-1}-1)}{2(p+1)}$$

of the intersections $M \cap M^g$ are such that $|M \cap M^g| = p+1$. Since for a fixed M the number of intersections $M \cap M^g$ is $\frac{p^r(p^r+1)(p^r-1)}{p(p-1)(p+1)} - 1$ and since

$$\begin{aligned}
1 + (p^{r-1}-1)(p+1) + \frac{p^2(p+1)(p^{r-1}-1)}{2(p-1)} + \frac{p^2(p-1)(p^{r-1}-1)}{2(p+1)} \\
= 1 + \frac{(p^{r-1}-1)(p^4+p^3+2p^2-p-1)}{p^2-1} \\
< \frac{p^r(p^r+1)(p^r-1)}{p(p-1)(p+1)},
\end{aligned}$$

there must exist a $g \in G$ such that $M \cap M^g = \{1_G\}$. ◻

COROLLARY 3.14. *Let $M = \mathrm{PGL}_2(p)$ be a maximal subgroup of G and $\mathcal{M}$ be the set of conjugates of M in G on which G acts by conjugation. Then the primitive action of G on $\mathcal{M}$ has the following non-trivial orbit lengths:*

a) $\frac{p^{r-1}-1}{p-1}$ *orbits of length* p^2-1,
b) $\frac{p\left(p^{r-1}-1\right)}{2(p-1)}$ *orbits of length* $p(p+1)$,
c) $\frac{p\left(p^{r-1}-1\right)}{2(p+1)}$ *orbits of length* $p(p-1)$,
d) $\frac{\left[\frac{p^r(p^r+1)(p^r-1)}{p(p-1)(p+1)}\right] - \left[1+\frac{(p^{r-1}-1)(p^4+p^3+2p^2-p-1)}{p^2-1}\right]}{p(p^2-1)}$ *orbits of length* $p(p^2-1)$.

PROOF. The proof follows by Lemma 2.6 and Theorem 3.13. ◻

The preceding lemmas, theorems and corollaries give the proof of Theorem 1.2 stated in Section 1.

ACKNOWLEDGEMENTS.

This work is based on the research supported by the National Research Foundation of South Africa (Grant Numbers 106071 and 120846). The authors would like to thank the anonymous referee for invaluable comments and observations which helped improve the presentation of the paper.

REFERENCES

[1] S. M. J. Amiri, *Maximum sum element orders of all proper subgroups of* $\mathrm{PGL}_2(q)$, Bull. Iranian Math. Soc. **39** (2013), 501–505.
[2] E. F. Assmus, Jr and J. D. Key, Designs and their codes, Cambridge University Press, Cambridge, 1992.
[3] A. Borovik and S. Yalçınkaya, *Construction of some subgroups in black box groups* $\mathrm{PGL}_2(q)$ *and* $\mathrm{PSL}_2(q)$, arXiv:1403.2224v1, (2014), `https://arxiv.org/abs/1403.2224`.
[4] P. J. Cameron, G. R. Omidi and B. Tayfeh-Rezaie, 3-*Designs from* $\mathrm{PGL}_2(q)$, The Electron. J. Combin. **13** (2006), #R50, 11 pp.
[5] D. Crnković and V. Mikulić, *Unitals, projective planes and other combinatorial structures constructed from the unitary groups* $U_3(q)$, $q = 3,4,5,7$, Ars Combin. **110** (2013), 3–13.

[6] D. Crnković, V. Mikulić and B. G. Rodrigues, *Designs, strongly regular graphs and codes constructed from some primitive groups*, in: Information security, coding theory and related combinatorics, IOS Press, Amsterdam, 2011, pages 231-252.
[7] M. R. Darafsheh, *Designs from the group* $\mathrm{PSL}_2(q)$*, q even*, Des. Codes Cryptogr. **39** (2006), 311–316.
[8] L. E. Dickson, Linear groups with an exposition of the Galois field theory, Dover Publications, Inc., New York, 1958.
[9] J. D. Dixon and B. Mortimer, Permutation groups, Springer-Verlag New York Inc., 1996.
[10] T. Fritzsche, *The depth of subgroups of* $\mathrm{PSL}_2(q)$ *II*, J. Algebra **381** (2013), 37–53.
[11] M. Giudici, *Maximal subgroups of almost simple groups with socle* $\mathrm{PSL}_2(q)$, `https://arxiv.org/abs/math/0703685`.
[12] J. D. Key and J. Moori, *Codes, designs and graphs from the Janko groups* J_1 *and* J_2, J. Combin. Math. Combin. Comput. **40** (2002), 143–159.
[13] J. D. Key and J. Moori, *Correction to "Codes, designs and graphs from the Janko groups* J_1 *and* J_2*", J. Combin. Math. Combin. Comput. 40 (2002), 143–159*, J. Combin. Math. Combin. Comput. **64** (2008), 153.
[14] J. D. Key, J. Moori and B. G. Rodrigues, *Permutation decoding for the binary codes from triangular graphs*, European J. Combin. **25** (2004), 113–123.
[15] O. H. King, *The subgroup structure of finite classical groups in terms of geometric configurations*, in: Surveys in combinatorics 2005, Cambridge Univ. Press, Cambridge, 2005, 29–56.
[16] X. Mbaale and B. G. Rodrigues, *Symmetric* 1*-designs from* $\mathrm{PSL}_2(q)$*, for q a power of an odd prime*, submitted.
[17] J. Moori, *Finite groups, designs and codes*, in: Information security, coding theory and related combinatorics, IOS Press, Amsterdam, 2011, 202–230.
[18] J. Moori and A. Saeidi, *Some designs invariant under the Suzuki groups*, Util. Math. **109** (2018), 105–114.
[19] J. Moori and A. Saeidi, *Constructing some designs invariant under* $\mathrm{PSL}_2(q)$, *q even*, Commun. Algebra **46** (2018), 160–166.
[20] R. A. Wilson, The finite simple groups, Springer-Verlag London Ltd., London, 2009.

X. Mbaale
School of Mathematics, Statistics and Computer Science
University of KwaZulu-Natal
Durban 4000, South Africa
E-mail: `xavier@aims.ac.za`

B. G. Rodrigues
Department of Mathematics and Applied Mathematics
University of Pretoria
Hatfield 0028, South Africa
E-mail: `bernardo.rodrigues@up.ac.za`

Received: 9.3.2020.